

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 16 AUG 2004

WIPO PCT



Applicant's or agent's file reference PCT-114	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/4-16)	
International application No. PCT/EP 02/04865	International filing date (day/month/year) 01.05.2002	Priority date (day/month/year) 01.05.2002
International Patent Classification (IPC) or both national classification and IPC H04L12/28		
Applicant TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

 These annexes consist of a total of 19 sheets.

- This report contains indications relating to the following items:
 - ☒ Basis of the opinion
 - ☐ Priority
 - ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - ☐ Lack of unity of invention
 - ☒ Reasoned statement under Rule 66.2(a)(II) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - ☐ Certain documents cited
 - ☐ Certain defects in the international application
 - ☐ Certain observations on the international application

Date of submission of the demand 27.11.2003	Date of completion of this report 13.08.2004
Name and mailing address of the International preliminary examining authority:  European Patent Office - Glitschiner Str. 103 D-10958 Berlin Tel. +49 30 25901 - 0 Fax: +49 30 25901 - 840	Authorized Officer RothlÜbbers, C Telephone No. +49 30 25901-478 

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP 02/04865

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-6 as originally filed
7-19 received on 13.02.2004 with letter of 11.02.2004

Claims, Numbers

1-25 received on 13.02.2004 with letter of 11.02.2004

Drawings, Sheets

1/4-4/4 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/EP 02/04865**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-23,25
	No: Claims	24
Inventive step (IS)	Yes: Claims	1-23,25
	No: Claims	24
Industrial applicability (IA)	Yes: Claims	1-25
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following document:

D1: US 2002/012433 A1 (EKBERG JAN-ERIK G ET AL) 31 January 2002 (2002-01-31)

2. Document D1 is considered to represent the most relevant state of the art, from which the subject-matter of claim 1 differs in that
- 2.1 the challenge-response authentication submissions in step c) take place before having provided IP connectivity to the user, and are carried:
- on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller; and
 - on an authentication protocol residing at application layer between the public land mobile network and the Access Controller; and
- the method further comprising the step of:
- (d) offering IP connectivity to the user at the wireless terminal, by sending an assigned IP address and other network configuration parameters, once said user has been validly authenticated by the public land mobile network,
- 2.2 The problem solved by these features may be regarded as how to overcome a lack of security caused by assigning an IP address to the wireless terminal in clear form before getting an agreement on applicable ciphering keys.
- 2.3 The solution to this problem proposed in independent claims 1 (method), 15 (Access Controller) and 25 (system) of the present application is considered as new and involving an inventive step (Article 33(3) PCT).
- 2.4 Claims 2-14 and 16-23 are dependent on claim 1 and 15 respectively and as such also meet the requirements of the PCT with respect to novelty and inventive step.
3. Claim 24 (wireless terminal) claims a wireless terminal that uses a PPPoE client and has an Extensible Authentication Protocol on top of this.
This does not reflect that the IP address is sent once said user has been validly

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 02/04865

authenticated by the public land mobile network. Thus an essential feature is missing and the claim is not clear in the sense of Article 6 PCT.

Furthermore, a wireless terminal having these features is already disclosed in document D1 (paragraph [0342]-[0350], where the PPP protocol is considered as equivalent to the PPPoE protocol).

Thus, claim 24 is not new (Article 33(2) PCT).

13. 02. 2004

allowing the operator to choose an encryption algorithm that better suites their security needs. Notice that there is usually a trade-off between security level and performance. Therefore, additional features like supporting
5 keys with a length of 128, 168, 256 bits, etc.; as well as supporting the latest most secure algorithms, like AES for instance, and a key rotation procedure may be considered another object of the present invention.

10 [0023] Moreover, in accordance with this application above, US 2002/0009199, the encrypted path goes from the Mobile Terminal to the AP, since WEP is only applicable to the radio path. In this respect, the support for an encryption path to be established beyond the AP, and covering also the wired part of the WLAN, is a further
15 object of the present invention.

[0024] Furthermore, US 2002/0009199 teaches that the assignment of an IP address is done before running the authentication process, and hence, a malicious user can potentially initiate a whole set of well-known attacks.
20 However, if a user had no means to get IP connectivity before having been effectively authenticated, the risk would decrease greatly. Thereby, it is a further object of the present invention the provision of an authentication mechanism for a user to be carried out before giving IP
25 connectivity to said user.

[0025] On the other hand, the applications US 2002/012433 and WO 01/76297 disclose, through some common exemplary embodiments, a system where a wireless adapted terminal can connect to a home mobile network through a Wireless IP
30 access network. The home mobile network being responsible for authenticating the user with a SIM-based authentication whereas the Wireless IP access network allowing the user to access to the Internet network once authenticated. The

REPLACEMENT SHEET

8

wireless terminal, the Wireless IP access network, and the mobile network all communicated with a mobile IP protocol. The system also comprises a Public Access Controller for controlling access from the radio access network to the Internet services. This Public Access Controller allocates an IP address to the wireless terminal and authenticates the wireless terminal before connection to the Internet is established, and relays authentication messages between the wireless terminal and the home mobile network. Moreover, the interface between wireless terminal and Public Access Controller is an IP based interface, wherein Public Access Controller and wireless terminal are identified by respective IP addresses from each other. The fact that Public Access Controller and wireless terminal make use of an IP-based protocol makes essential that the wireless terminal is assigned an IP address from the very beginning, this IP address sent from the Public Access Controller to the wireless terminal before establishing a secure channel communication. Thereby, the same problem as with the above application, US 2002/0009199, occurs due to the fact that the assignment of an IP address is done before running the authentication process, and hence, a malicious user can potentially initiate a whole set of well known attacks.

[0026] In summary, an important object of the present invention is the provision of a system, means and methods for allowing an effective SIM-based user authentication and for establishing a complete encryption path, starting from the TE, for WLAN users who are subscribers of a public land mobile network. Another particularly important object is that this SIM-based user authentication might be performed before giving IP connectivity to said user.

REPLACEMENT SHEET

9

[0027] A further object of the present invention is the support of keys of variable length, the use of security algorithms at operator choice, and provision of a key rotation procedure.

- 5 [0028] A still further object of the present invention is the achievement of the previous objects with a minimum impact on conventional WLAN scenarios.

SUMMARY OF THE INVENTION

- 10 [0029] The objects of the invention are achieved with a method for allowing a SIM-based authentication to users of a wireless local area network who are subscribers of a public land mobile network by means of a data link layer (layer-2) authentication mechanism. An important aspect of this method is that the IP connectivity is only provided to
15 the user when the authentication process has been successfully completed.

- [0030] The objects of the invention are thus achieved with a method wherein a wireless terminal finds an accessible Access Point and requests association to the wireless local
20 area network, and the Access Point accepts the request for that. The wireless terminal then initiates the discovering of an Access Controller interposed between the Access Point and the public land mobile network.

- [0031] Then, the wireless terminal sends the user
25 identifier immediately on top of a Point-to-Point layer 2 protocol toward the Access Controller which shifts the user identifier received on top of a Point-to-Point layer 2 protocol upwards to an authentication protocol residing at application layer.

- 30 [0032] Following, the Access Controller sends the user identifier toward an Authentication Gateway at the public

REPLACEMENT SHEET

10

land mobile network to initiate an authentication procedure.

[0033] Once, the authentication process is starting the Access Controller receives an authentication challenge from the public land mobile network via the Authentication Gateway; and shifts the authentication challenge received on the same protocol at application layer downwards on top of the Point-to-Point layer 2 protocol. The authentication challenge is sending by the Access Controller toward the wireless terminal for deriving an authentication response.

[0034] Then, the wireless terminal can send the authentication response immediately on top of a Point-to-Point layer 2 protocol toward the Access Controller which shifts the authentication response received on top of a Point-to-Point layer 2 protocol upwards to the authentication protocol at application layer. The authentication response is sending toward the Authentication Gateway from the Access Controller that receives an encryption key from the public land mobile network via the Authentication Gateway.

[0035] Following, the Access Controller extracts the encryption key received on the protocol at application layer for further encryption of communication path with the wireless terminal; and the Access Controller sends an assigned IP-address and other network configuration parameters toward the wireless terminal.

[0036] This provides the advantages that the mobile terminal adds security authentication mechanism, similar to the ones used in radio communication network, in overall communication path; this means that it obtains confidentiality in wireless path and in wire path. The operators can extend their access networks, offering localized broadband access (11 Mbps) at a very low cost.

REPLACEMENT SHEET

11

[0037] Also for accomplishing the objects of the present invention there is provided an Access Controller that comprises a Point-to-Point server residing at an OSI layer-2 for communicating with the wireless terminal; and an authentication protocol residing at an OSI application layer for communicating with the public land mobile network. Moreover, this Access Controller further comprises means for shifting the information received on top of the Point-to-Point layer-2 protocol upwards to an appropriate authentication protocol residing at application layer. Likewise, the Access Controller also comprises means for shifting the information received on the authentication protocol residing at application layer downwards on top of the Point-to-Point layer 2 protocol.

[0038] In order to fully accomplish the objects of the invention, it is also provided a wireless terminal comprising functionality for acting as a Point-to-Point layer 2 protocol client and having an Extensible Authentication Protocol on top of this Point-to-Point layer 2 protocol.

[0039] The overall solution provided by the invention results in a telecommunication system comprising a wireless local area network that includes at least one Access Point, a public land mobile network, at least one wireless terminal as above, and the Access Controller above.

BRIEF DESCRIPTION OF DRAWINGS

[0040] The features, objects and advantages of the invention will become apparent by reading this description in conjunction with the accompanying drawings, in which:

[0041] FIG. 1 represents a preferred embodiment of how a user of a conventional mobile network accessing through a

REPLACEMENT SHEET

12

WLAN, which can be accessed by mobile and non-mobile users, may be authenticated by his own mobile network and may have an encrypted path from the TE to his own mobile network.

5 [0042] FIG. 2 presents a simplified architecture compared to the one in Fig. 1, and applicable to a WLAN accessed only by users of a public land mobile network.

10 [0043] FIG. 3 schematically shows an embodiment of an Access Controller comprising a PPPoE Server and a RADIUS Client wherein the Extensible Authentication Protocol resides.

[0044] FIG. 4 basically shows an exemplary sequence of actions carried out from the TE to the mobile network and throughout the WLAN entities to perform a SIM-based user authentication.

15 **DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS**

[0045] The following describes currently preferred embodiments of means, methods and system for allowing an effective SIM-based user authentication and for establishing a complete encryption path starting from the
20 TE for WLAN users who are subscribers of a public land mobile network. In accordance with an aspect of the present invention, this SIM-based user authentication is performed before having given IP connectivity to said user.

[0046] Therefore, an overall sketch of a preferred
25 embodiment is presented in Fig. 1, showing a general scenario where subscribers of a public land mobile network (GSM/GPRS/UMTS), as well as other local non-mobile users, access a wireless local area network (WLAN). This general scenario in Fig. 1 proposes a particularly simple
30 architecture aimed to minimise the impacts on an existing conventional WLAN in order to accomplish one of the objects

REPLACEMENT SHEET

13

of the present invention. This rather simple architecture involves different entities from a WLAN and from a public land mobile network, which are described following this. Moreover, Fig. 2 presents an even more simplified architecture in accordance with another embodiment of the present invention for a WLAN giving access only to subscribers of a public land mobile network and without local WLAN users.

[0047] A first entity in Fig. 1 and 2 is the Terminal Equipment (TE), that is equipped with the necessary hardware and software to interface the user's SIM card as well as to send and receive the required signalling information according to the Authentication and Key Agreement (AKA) protocol. The TE also includes the necessary software to implement a Point-to-Point Protocol over Ethernet (PPPoE) protocol, client side, accordingly with RFC 2516.

[0048] The inclusion of such PPPoE client allows the establishment of a Point-to-Point Protocol (PPP) session with a specific server in the WLAN domain. This is a very convenient embodiment in order to leverage on existing authentication mechanisms, for instance the Extensible Authentication Protocol (EAP), and on encryption protocols, like the PPP Encryption Control Protocol (hereinafter referred to as "PPP encrypted") according to RFC 1968, that extends the encryption path along the wired part of the WLAN, thus offering a much higher security level. A component like this PPPoE Client is a core part for the proposed solution.

[0049] Other entities in the scenarios in Fig. 1 and 2 are the Access Points that behave as plain standard radio stations according to the standard 802.11b, without any additional logic. Unlike other possible solutions, as

REPLACEMENT SHEET

14

explained in respect of the coming standard 802.1x, the approach offered by the present invention allows the reuse of the cheap existing hardware instead of having to replace or upgrade all AP's present in the WLAN. These unchanged
5 AP's might run in this scenario with WEP support turned off, since such WEP offers by itself a little security compared to the security mechanisms that are implemented on top of the PPPoE layer.

[0050] In accordance with an aspect of the present
10 invention, there is provided a new entity, the Access Controller (hereinafter referred to as AC) in both Fig. 1 and 2 that comprises the required PPPoE server functionality. This PPPoE server is automatically discovered by the Terminal Equipment (TE), by means of a
15 built-in mechanism in the PPPoE protocol, namely through a handshake initiated by a broadcast message. This Access Controller (AC) also comprises a RADIUS client functionality that has the responsibility of gathering client credentials, received through EAP attributes carried
20 on top of a PPP, and sending them toward a conventional WLAN Authentication Server (WLAN-AS), also through EAP attributes carried now on top of RADIUS messages. A component like this Access Controller (AC) is also a core part for the purpose of the present solution.

25 [0051] Both the Access Controller and the aforementioned PPPoE client, which is embedded in the Terminal Equipment, are co-operating entities intended for tunnelling a challenge-response authentication procedure as well as for establishing an encrypted path.

30 [0052] A further entity present only in the most general scenario shown in Fig. 1 is a WLAN-Authentication Server (WLAN-AS) that implements the functionality of a local authenticator server for local WLAN users, not belonging to

REPLACEMENT SHEET

15

the mobile operator, and who may be thus authenticated by other means such as a plain user and password matching. This WLAN-AS also plays the role of a RADIUS proxy, when receiving authentication messages from the Access
5 Controller and forwards them toward an Authentication Gateway (hereinafter referred to as AG) in the public land mobile network operator's domain.

[0053] The WLAN-AS is only required for the purpose of the present invention in order to authenticate own WLAN users
10 who are not mobile subscribers of the public land mobile network. Consequently, a WLAN intended for giving access only to subscribers of a mobile network may get rid of such entity without affecting the authentication of said mobile subscribers and the establishment of an encrypted path,
15 scope of the present invention. In this respect, Fig. 2 presents an embodiment of a simplified architecture for a WLAN giving access only to subscribers of a public land mobile network as explained above wherein the WLAN-AS is thus not included.

20 [0054] A still further entity included in the scenarios of Fig. 1 and 2 is the Authentication Gateway (hereinafter referred to as AG) alone or likely in co-operation with a Home Location Register (HLR) for storing mobile subscribers user data. This Authentication Gateway (AG), alone or in
25 combination with an HLR, act as authentication backend servers inside the operator's domain, and are in charge of generating authentication vectors according to the AKA protocol for conventional and newer public land mobile networks such as GSM, GPRS and UMTS. These components,
30 namely AG and HLR, can be physically separate entities which communicate each other by the Mobile Application Part (MAP) protocol, or they can be a single logical entity acting as a RADIUS server and with the subscriber database built-in, together with the implementation of the necessary

REPLACEMENT SHEET

16

algorithms in AKA, such as the well-known A5, A8 and so on. In the latter approach, the communication toward an HLR is, hence, not needed as exemplary illustrated in Fig. 2.

- [0055] In short, the Access Controller, the aforementioned
5 PPPoE client, which is embedded in the Terminal Equipment, and this Authentication Gateway are the core entities for the purpose of the present invention. The particular description for the functions residing in such entities is merely illustrative and in non-restrictive manner.
- 10 [0056] Fig. 3 shows different protocol layers involved in an Access Controller (AC) with reference to the Open System Interconnection (OSI) model. The PPPoE server, residing underneath an IP layer, comprising a PPPoE protocol layer that naturally resides over an Ethernet layer, and having
15 embedded the aforementioned EAP. Likewise, the RADIUS client having a RADIUS protocol layer having embedded the EAP, residing over an UDP layer, both residing over an IP layer.

- [0057] On the other hand, the manner in which the
20 different elements carry out some aspects of the present invention accordingly with currently preferred embodiments is described below with reference to the sequence of actions depicted in Fig. 4.

- [0058] The aforementioned Terminal Equipment (TE) is
25 equipped with a Mobile Terminal Adapter (MTA) that allows the access to a SIM card carried by a mobile terminal. This TE has a transceiver for communicating (C-401, C-402) with an AP of the WLAN, and includes the appropriate software stack to implement the PPPoE protocol in accordance with
30 the RFC 2516.

- [0059] The Access Controller (AC) has a PPPoE server embedded. The discovery of the PPPoE server by the PPPoE

REPLACEMENT SHEET

17

client is an integral part of the protocol itself (C-403, C-404, C-405, C-406). The identity used by the TE on the PPP link (C-407, C-408) is a Network Access Identifier (NAI), which is entered by the user for establishing
5 required dial-up sessions, and whose realm is used to identify the user as a subscriber of a given mobile operator. No password is needed since the authentication is done by other means. Alternatively, instead of sending a NAI, the IMSI could be fetched from the SIM card and sent
10 as the user identity. This should only be used if sending the IMSI in clear-text is acceptable, which might not be the case.

[0060] Having received the user identity with help of EAP mechanisms, the Access Controller (AC) has a RADIUS client
15 for sending (C-409) authentication messages to the WLAN-AS server. The Extensible Authentication Protocol (EAP) is run on top of PPP and RADIUS, in order to carry authentication information between the TE and the AG. The authentication mechanism to be used inside EAP may be the conventional AKA
20 used in public land mobile networks. As already mentioned above, the WLAN-AS acts as an authentication server for regular WLAN users, whose authentication is not SIM-based, and as an authentication proxy for those users whose realm part of the NAI identifies them as subscribers of a mobile
25 network thus using a SIM-based authentication. Then, when acting as an authentication proxy, the WLAN-AS forwards (C-410) the received authentication messages to the Authentication Gateway (AG).

[0061] When the Authentication Gateway receives (C-410) an
30 authentication request, asks the HRL for an authentication vector (C-411), triplet or quintet, by using a MAP interface. For this task, the Authentication Gateway (AG) has to know the IMSI of the subscriber whose NAI have been sent in the RADIUS message. This IMSI may be discovered by

REPLACEMENT SHEET

18

lookup in a directory database, for instance. The HLR answers back with the requested authentication information (C-412) for the user.

5 **[0062]** Then, the AG encapsulates the RAND component of the authentication vector in an EAP attribute and sends it back through the WLAN-AS (C-413) toward the AC (C-414) inside a RADIUS message. Notice that for user of newer mobile networks like UMTS, the sending of a message like AUTN might also be required.

10 **[0063]** The AC then forwards (C-415) the received EAP information to the TE in a PPP message. Notice that the AC behaves here as a "passthrough" of EAP information between "carrier" protocols such as PPP and RADIUS.

15 **[0064]** When the TE receives the EAP information, extracts the RAND number and uses it to challenge the SIM and generate an answer (RES), that is sent back (C-416, C-417, C-418) to the AG via EAP transmitted over PPP and RADIUS again. As before, for UMTS users the TE first authenticates the network, based on the AUTN. At this stage, it has to be
20 noticed that the TE generates the encryption key following the standard algorithms defined in AKA. This key is used as a seed, namely keying material, to derive one or multiple session keys to be used with the PPP Encryption Control Protocol stated in RFC 1968, and any of the existing PPP
25 encryption algorithms, for instance, the PPP triple-DES encryption protocol, RFC 2420.

30 **[0065]** The AG receives (C-418) the EAP response and checks the validity of the challenge. The AKA encryption key (Kc) had been received previously in the authentication vector from the HLR likely in co-operation with an Authentication Centre (AuC) not depicted. The AG communicates then the AKA encryption key (Kc) to the AC (C-419, C-420) where the PPPoE server resides. This may be done in an Access-Accept

REPLACEMENT SHEET

19

RADIUS message where the EAP-Success is transmitted, but since this EAP command cannot carry any additional data, a RADIUS Vendor Specific Attribute (VSA) may be a more valuable option.

- 5 [0066] At this stage, the AC receives (C-420) an Access-Accept RADIUS message and requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server, this IP address to be further sent to the TE. The AC follows the same algorithm as the TE to derive session keys from the
- 10 AKA encryption key (Kc) to be used with the PPP Encryption Control Protocol and the chosen PPP encryption algorithm (3DES, for instance). The AC eventually sends (C-421) the EAP-success message to the TE, together with other configuration parameters destined to said TE, such as an IP
- 15 address, an IP net mask, DNS servers, and so on. Then, the PPP link is fully established and ready to enter the network phase.

REPLACEMENT SHEET

20

CLAIMS

1. A method in a telecommunication system for allowing a
SIM-based authentication to users of a wireless local
area network who are subscribers of a public land
mobile network, the method comprising the steps of:

- 5 (a) a wireless terminal accessing the wireless local
area network through an accessible Access Point;
- 10 (b) discovering an Access Controller interposed between
the Access Point and the public land mobile network
from the wireless terminal;
- 15 (c) carrying out a challenge-response authentication
procedure between the wireless terminal and the
public land mobile network through the Access
Controller, the wireless terminal provided with a
SIM card and adapted for reading data thereof;

the method **characterized in that** the challenge-response
authentication submissions in step c) take place
before having provided IP connectivity to the user, and
are carried:

- 20 - on top of a Point-to-Point layer 2 protocol
(PPPoE) between the wireless terminal and the
Access Controller; and
- on an authentication protocol residing at
application layer between the public land
mobile network and the Access Controller; and
- 25

the method further comprises a step of:

- (d) offering IP connectivity to the user at the
wireless terminal, by sending an assigned IP
address and other network configuration parameters,

REPLACEMENT SHEET

21

once said user has been validly authenticated by the public land mobile network.

2. The method in claim 1, wherein the step b) of discovering an Access Controller includes a step of establishing a Point-to-Point Protocol session between a Point-to-Point over Ethernet (PPPoE) Protocol client in the wireless terminal and a Point-to-Point over Ethernet (PPPoE) Protocol server in the Access Controller.
3. The method in claim 1, wherein the step c) of carrying out the challenge-response authentication procedure include the steps of:
- (c1) sending a user identifier from the wireless terminal to the public land mobile network through the Access Controller;
 - (c2) receiving an authentication challenge at the wireless terminal from the public land mobile network via the Access Controller;
 - (c3) deriving encryption key and authentication response at the wireless terminal from the received challenge;
 - (c4) sending the authentication response from the wireless terminal to the public land mobile network through the Access Controller;
 - (c5) receiving at the Access Controller an encryption key from the public land mobile network; and
 - (c6) extracting the encryption key received for further encryption of communication path with the wireless terminal.

REPLACEMENT SHEET

22

4. The method in claim 2, further comprising a step of shifting authentication information received on top of a Point-to-Point layer 2 protocol (PPPoE) upwards to an authentication protocol residing at application layer
5 for submissions toward the public land mobile network.
5. The method in claim 4, further comprising a step of shifting authentication information received on an authentication protocol residing at application layer downwards on top of a Point-to-Point layer 2 protocol
10 (PPPoE) for submissions toward the wireless terminal.
6. The method in claim 3, further comprising a step of establishing at the wireless terminal a symmetric encryption path by using the previously derived encryption keys at the Access Controller and wireless
15 terminal.
7. The method in any preceding claim, wherein the step d) of sending an IP address includes a previous step of requesting such IP address from a Dynamic Host Configuration Protocol server.
- 20 8. The method in any preceding claim, wherein the communication between the Access Controller and the public land mobile network goes through an Authentication Gateway of said public land mobile network.
- 25 9. The method in any preceding claim, wherein the communication between the Access Controller and the Authentication Gateway of a public land mobile network goes through an Authentication Server of the wireless local area network in charge of authenticating local
30 users of said wireless local area network who are not mobile subscribers.

REPLACEMENT SHEET

23

10. The method in any preceding claim, wherein the user identifier in step c1) comprises a Network Access Identifier.
- 5 11. The method in any preceding claim, wherein the user identifier in step c1) comprises an International Mobile Subscriber Identity.
12. The method in any preceding claim, wherein the authentication protocol residing at application layer in step c) is an Extensible Authentication Protocol.
- 10 13. The method in claim 12, wherein this Extensible Authentication Protocol is transported over a RADIUS protocol.
14. The method in claim 12, wherein this Extensible Authentication Protocol is transported over a Diameter protocol.
- 15 15. An Access Controller in a telecommunication system that comprises a wireless local area network including at least one Access Point, a public land mobile network, and at least one Terminal Equipment provided with a SIM card and adapted for reading subscriber data thereof, the Access Controller **characterized in that** it comprises:
- 20 (a) a Point-to-Point layer 2 protocol (PPPoE) server for communicating with the wireless terminal, and arranged for tunneling the challenge-response authentication procedure; and
- 25 (b) an authentication protocol residing at an OSI application layer for communicating with the public land mobile network.
- 30 16. The Access Controller in claim 15 further comprising:

REPLACEMENT SHEET

24

- (a) means for shifting the information received on top of the Point-to-Point layer 2 protocol (PPPoE) upwards to the authentication protocol residing at application layer; and
- 5 (b) means for shifting the information received on the authentication protocol residing at application layer downwards on top of the Point-to-Point layer 2 protocol (PPPoE).
- 10 17. The Access Controller in claim 16 further comprising means for requesting an IP address from a Dynamic Host Configuration Protocol server, after a user has been successfully authenticated by his public land mobile network.
- 15 18. An Access Controller according to claim 17 adapted for communicating with a wireless terminal via an Access Point.
19. An Access Controller according to claim 17 adapted for communicating with a public land mobile network via an Authentication Gateway.
- 20 20. An Access Controller according to claim 17 adapted for communicating with an Authentication Gateway via an Authentication Server responsible for authenticating local users of a wireless local area network.
- 25 21. An Access Controller according to any of claims 15 to 20, wherein the authentication protocol residing at application layer is an Extensible Authentication Protocol.
- 30 22. The Access Controller in claim 21, wherein this Extensible Authentication Protocol is transported over a RADIUS protocol.

REPLACEMENT SHEET

25

23. The Access Controller in claim 21, wherein this Extensible Authentication Protocol is transported over a Diameter protocol.
- 5 24. A wireless terminal comprising functionality for acting as a Point-to-Point layer 2 protocol (PPPoE) client and having an Extensible Authentication Protocol on top of this Point-to-Point layer 2 protocol.
- 10 25. A telecommunication system comprising a wireless local area network that includes at least one Access Point, a public land mobile network, and at least one Terminal Equipment provided with a SIM card and adapted for reading subscriber data thereof, **characterized in that** it further comprises the Access Controller in claims 15 to 23 for allowing SIM-based subscriber authentication to users of the wireless local area network who are
- 15 subscribers of the public land mobile network.